International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 1, Feb 2015, 67-74

ENHANCED UNIFIED AUTHENTICATION AND AUTHORIZATION ARCHITECTURE BASED ON DESKTOP VIRTUALIZATION

KIRANKUMAR GAIKWAD[1], RUPALI NIKHARE[2] & RAHUL JIWANE[3]

[1]Department of Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India

[2]Department of Computer Engineering, Pillai Institute of Information Technology, Engineering, Media Sudies & Research, Maharashtra, India

[3]Department of Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India

ABSTRACT

Virtualization is one of the fundamental technologies that makes cloud computing work. However, virtualization is not cloud computing. Increase in use of Desktop Virtualization has become quite difficult to centrally manage user's authentication and authorization in unified mode. In this paper we will analyze the existing unified authentication architecture and then see the implementation of enhanced unified authentication and authorization architecture. Further we will compare advantages and disadvantages of both the systems.

KEYWORDS: Desktop Virtualization, Single Sign On, Desktop Cloud, Oauth

INTRODUCTION

Virtualization and cloud computing were both developed to maximize the use of computing resources while streamlining processes and increasing efficiencies to reduce the total cost of ownership. While we frequently hear people discuss these two terms interchangeably, they are truly very different approaches to solve the problem of maximizing the use of available resources which leads to some important considerations when selecting between the two. The technology of unified authentication or single sign on (SSO) is still under improvement. Tim Mather, etc. thought that cloud computing certifications include authentication, authorization, auditing, and identity federation management, technology. They described the identity life cycle management of all stages in Figure 1.[1]

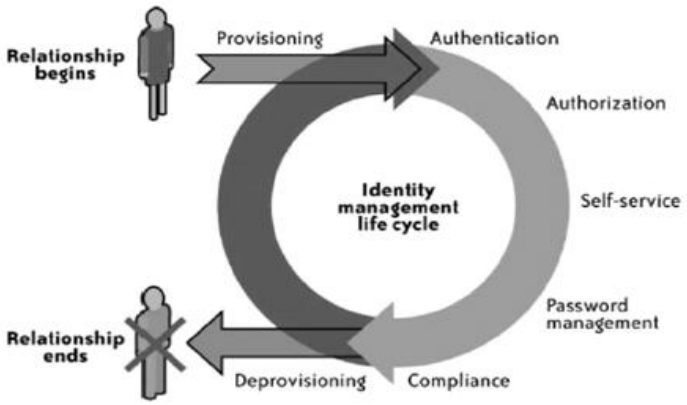

Figure 1: Identity Life Cycle

In figure 1 user gets the provision by authenticating, using username and password. According to the authorities provided, user uses the self service application. User need to authenticate their identities each time while using each application and service. They are also able to manage password and compliance according to the specific standard. This type of process have disadvantages like, increase in password fatigue, time consumption by retyping password and increase in IT cost to maintain all username & password. Therefore, single sign on (SSO) or unified authentication has become a good choice for desktop virtualization and cloud computing environment.

The architecture of desktop cloud authentication is generally like that shown in Figure 2. In this architecture, the unified authentication management module authenticates user'sidentitieswhen they get access to the desktop cloud system by the user portal. Authorization application and management module authorize the user based on the user information in the user info database. Then users can get access to the applications and services within the range of their rights. The advantage of this architecture is to achieve a single sign-on and to provide the user a good user experience. With this architecture users need not login for multiple times and to provide their information for each and every applications or services. At the same time, the architecture effectively prevents unauthorized access to applications or services by centralizing user authentication and access management. Thus the security of the desktop cloud system is significantly improved.[2]

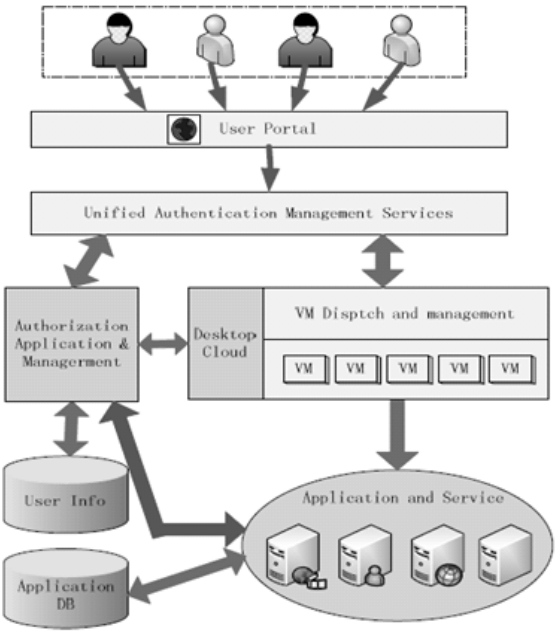

Figure 2: Desktop Cloud General IdentityAuthentication Architecture

METHODS

The idea of Enhanced Unified Authentication and Authorization Architecture was first proposed by Sun Yongqing, Zou Xiang in "Desktop Cloud-based Research on Unified Authentication Architecture", 978-1-4577-1964-6/12 ©2012 IEEE as shown in figure 3. But according to the authors "The proposed architecture can achieve the desktop cloud unified authentication in theory, but they haven't tested its advantages and disadvantages in practical application. To design more general and more comprehensive desktop cloud unified authentication model, need of more efforts from the circles of academia and industry are required."[2]

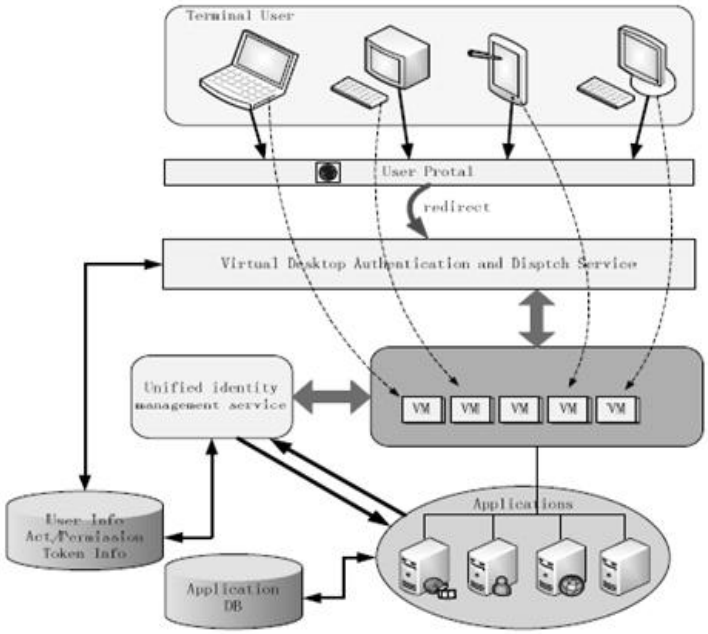

Figure 3: Desktop Cloud Identity Authentication Architecture Based Application

We have successfully implemented the above system with some small significant changes. Figure 4 shows the flow of project, where the end user is able to sign-in to 2 different servers- Image Server and Document Server by use of Authentication Server. Instead of using different applications we are using images and documents files. Authentication Server contains virtual machines (VM) for respective users and are only assigned after proper authentication. Authentication Server is connected to the User Database to access the user information. All the computer are connected in network. The registeration process of user is kept with System Administrator for security reasons.

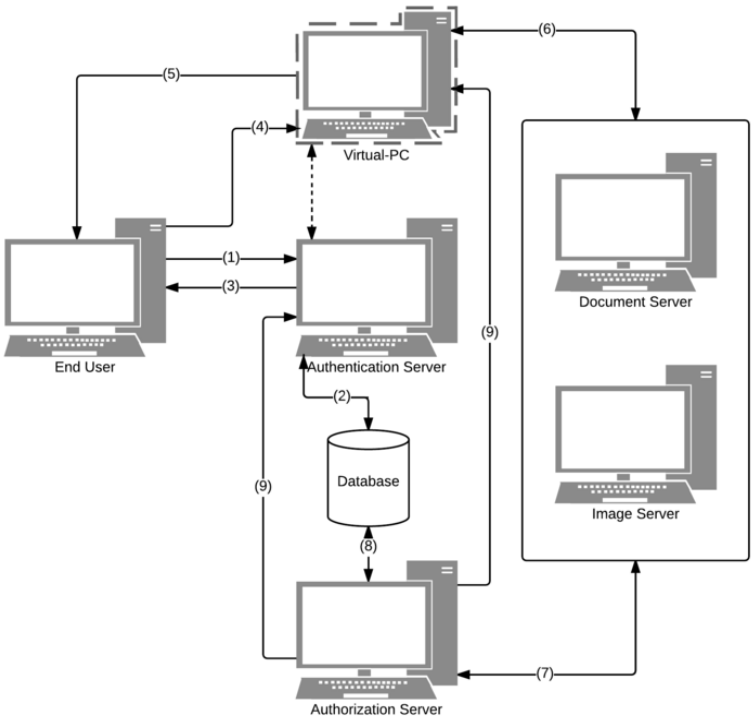

Figure 4: Flow of Enhanced Unified Authentication and Authorization Architecture

Flow of the Project

Step 1: End User uses given credentials to log into the system. The request is send to the Authentication Server. To make the system more secure we have used md5 algorithm to encrypt the user credential.

Step 2: Authentication Server will authenticate if the user is valid, using the User Info Database. If valid, then user will be permitted to log in. If not, user will be restricted from loging into the system. It is nothing but Virtual Desktop Authentication and Dispatch Service as shown in the proposed system figure 3. By using MySql on network, uses SSL Protocol to maintain strong secure data.

Step 3: After aunthenticating, user will see connection information of the user and will be ready to use the VM.

Step 4: When the user clicks on START, using Virtual Network Computing (VNC) he will be able to access the Virtual Machine. VNC uses Remote Buffer Protocol to connect the client machine and VM.

Step 5: Each user has its own VM on Authentication Server, created at the time of user registration process. By default these VM's reside in Authentication Server and later assigned to the user.

Step 6: After accessing the VM that is assigned by Authentication Server, user is able to access Image Server and Document Server.

Step 7: When user enters in respective Server, he will be able to access normal images or documents. But will be restricted to protected files. To access these files user will raise a request for token and send to Authorization Server. Authorization Server will generate a token. This server is same as Unified Identity Management Service as shown in proposed system figure 3.

Step 8: The token generated by Authorization Server is saved in the Database, which can be further used by both Authentication Server and Authorization Server.

Step 9: Same token will be send to VM that has requested for a token. But this token will be delivered only if, the client answer's the security question asked by Authorization Server, making the system more secure. This server will check the answer in the user info database and then deliver the token.

Step 10: Authentication Server will check both the token i.e one which is saved in database and other which is send to VM. If both the tokens match then user will be able to access the protected files. This Process is similar to OAuth i.e Open standard to Authorization.

RESULTS

Step 1: End user logs into Authentication Server using credentials.

Figure 5

Step 2: Entering Invalid credential will restrict the user to access further.

Figure 6

Step 3: If valid user, then he will see connection information of the user.

Figure 7

Step 4: After clicking on START, with help of VNC, user will access Virtual Machine.

Figure 8

Step 5: VM assigned to the user.

Figure 9

Step 6: After accessing the VM that is assigned by Authentication Server, user is able to access Image Server and Document Server.

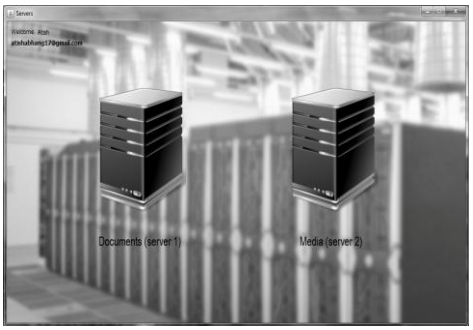

Figure 10

Step 7: Raise a request to Authorization Server to access protected files.

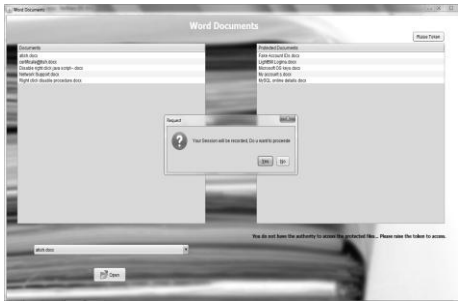

Figure 11

Step 8: Token saved in database for future use.

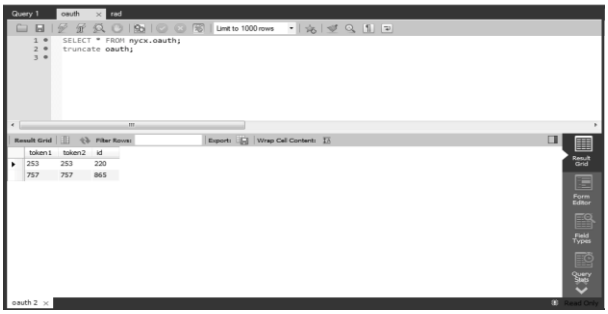

Figure 12

Step 9: Security questions asked to VM before delivering token.

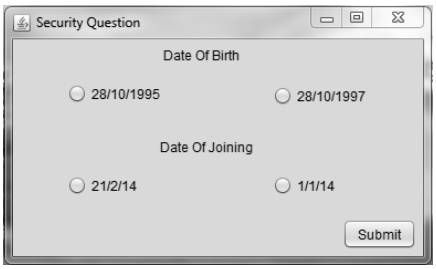

Figure 13

Step 10: Access the files after process of token matching.

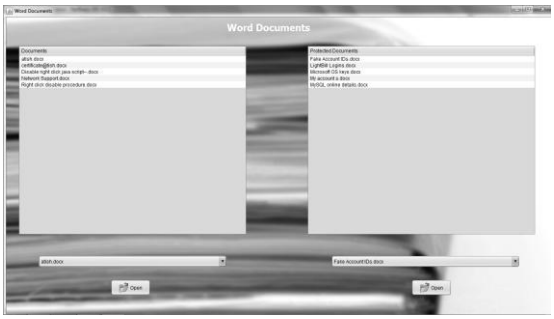

Figure 14

CONCLUSIONS

New Implemented system has the following advantages over the existing System.

- Easy to implement as compared to existing systems.
- Privilege management or Authorization Management is included which is not present in existing systems.
- Run-time management of services i.e. Addition and removal of service is possible in this architecture.

This architecture has achieved the desktop cloud unified authentication in theory and practical. To design more general and more comprehensive desktop cloud unified authentication model, weneed more cost and effort. Thuswe have achievedour goal to implement a desktop cloud system using the proposed architecture.

ACKNOWLEDGEMENTS

Authors are greatful and thankful to Mr. Atish S. Abhang for assistance to carry out this research work**.**

REFERENCES

1. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security andPrivacy. O'REILLY, pp. 77-80.
2. Sun Yongqing and Zou Xiang, "Desktop Cloud-based Research on Unified Authentication Architecture", 978-1-4577-1964-6/12 ©2012 IEEE**.**